Y. Kitaoka
Nagoya Math. J.
Vol. 69 (1978), 117-120

REPRESENTATIONS OF QUADRATIC FORMS

YOSHIYUKI KITAOKA

0. We have shown in [1]

THEOREM A. *Let L be a lattice in a regular quadratic space U over $\boldsymbol{Q}$; then L has a submodule M satisfying the following conditions* 1), 2):

1) $dM \neq 0, \operatorname{rank} M = \operatorname{rank} L - 1$, *and M is a direct summand of L as a module.*

2) *Let L' be a lattice in some regular quadratic space U' over $\boldsymbol{Q}$ satisfying $dL' = dL$, $\operatorname{rank} L' = \operatorname{rank} L$, $t_p(L') \geq t_p(L)$ for any prime p. If there is an isometry α from M into L' such that $\alpha(M)$ is a direct summand of L' as a module, then L' is isometric to L.*

Our aim is to remove such a restriction in 2) that $\alpha(M)$ is a direct summand of L' as a module:

THEOREM B. *Let L be a lattice in a regular quadratic space U over $\boldsymbol{Q}$; then L has a submodule M with $\operatorname{rank} M = \operatorname{rank} L - 1$, $dM \neq 0$ which is a direct summand of L as a module and satisfies*

(*) *let L' be a lattice in some regular quadratic space U' over $\boldsymbol{Q}$ satisfying $dL' = dL$, $\operatorname{rank} L' = \operatorname{rank} L$, $t_p(L') \geq t_p(L)$ for any prime p; if there is an isometry α from M into L', then L' is isometric to L.*

1. Notations and some lemmas

We denote by $\boldsymbol{Q}, \boldsymbol{Z}, \boldsymbol{Q}_p$ and $\boldsymbol{Z}_p$ the rational number field, the ring of rational integers, the p-adic completion of $\boldsymbol{Q}$, and the p-adic completion of $\boldsymbol{Z}$, respectively. For a quadratic space U we denote $Q(x), B(x, y)$ the quadratic form and the bilinear form associated with U ($2B(x, y) = Q(x + y) - Q(x) - Q(y)$), and for a lattice L in U dL stands for the discriminant of L. For two ordered sets $(a_1, a_2, \cdots, a_n)$, $(b_1, b_2, \cdots, b_n)$, we define the order $(a_1, a_2, \cdots, a_n) \leq (b_1, b_2, \cdots, b_n)$ by either $a_i = b_i$ for $i < k$ and $a_k < b_k$ for some $k \leq n$ or $a_i = b_i$ for any i.

Received February 18, 1977.

https://doi.org/10.1017/S0027763000017979 Published online by Cambridge University Press

Let L be a lattice in a regular quadratic space over $\boldsymbol{Q}_p$; then L has a Jordan splitting $L = L_1 \perp L_2 \perp \cdots \perp L_k$, where L_i is a p^{a_i}-modular lattice and $a_1 < a_2 < \cdots < a_k$. We denote by $t_p(L)$ the ordered set $(\underbrace{a_1, \cdots a_1}_{\operatorname{rank} L_1}, \cdots, \underbrace{a_k, \cdots, a_k}_{\operatorname{rank} L_k})$. For a lattice L in a regular quadratic space over $\boldsymbol{Q}$ we abbreviate $t_p(\boldsymbol{Z}_pL)$ to $t_p(L)$.

LEMMA 1. *Let L be a lattice in a regular quadratic space U over $\boldsymbol{Q}_p$; then L has a submodule M satisfying the following conditions:*

1) *$dM \neq 0$, $\operatorname{rank} M = \operatorname{rank} L - 1$, and M is a direct summand of L as a module.*

2) *Let L' be a lattice in U containing M; then $L' = L$ if $dL' = dL$ and $t_p(L') \geq t_p(L)$.*

This was proven in [1], and we called M a characteristic submodule of L.

LEMMA 2. *Let L be a lattice with the scale $\subset \boldsymbol{Z}$ in a regular quadratic space U over $\boldsymbol{Q}$ with $\dim U \geq 3$. If a direct summand M of L satisfies*

1) *M_p is a characteristic submodule of L_p if $p \mid 2dL$,*

2) *$dM = q^r m$ where q is a prime with $q \nmid 2dL$ and $r \geq 0$, and $p \mid 2dL$ if $p \mid m$,*

then M satisfies the conditions 1), 2) in Theorem A.

This is a remark in §1 in [1].

LEMMA 3. *Let L be a lattice in a regular quadratic space U over $\boldsymbol{Q}$ with $\dim U > 2$, and let S be a finite set of finite primes such that $2 \in S$, and L_p is unimodular for $p \notin S$. For a given $u_p \in L_p (p \in S)$ there is a prime $q \notin S$ and a vector $u \in L$ such that u and u_p are sufficiently near for $p \in S$, and $Q(u) \in \boldsymbol{Z}_p^\times$ for $p \neq q, p \notin S$, and $Q(u) \in q\boldsymbol{Z}_q^\times$.*

Proof. We can take a vector v_1 in L such that v_1 is sufficiently near to u_p for $p \in S$ and $Q(v_1) \neq 0$, and put $T = \{p; p \notin S, Q(v_1) \notin \boldsymbol{Z}_p^\times\}$. Then there is a vector $v_2 \in L$ such that $Q(v_2) \in \boldsymbol{Z}_p^\times$ for $p \in T$ and $\pm d\boldsymbol{Z}[v_1, v_2]$ is not in $\boldsymbol{Q}^{\times 2}$ since L_p is unimodular for $p \notin S$. Put $\tilde{L} = \boldsymbol{Z}[v_1, v_2] \subset L$, and take a vector v in $\tilde{L}$ such that v and v_1 (resp. v_2) are sufficiently near for $p \in S$ (resp. $p \in T$). There is a basis $\{e_1, e_2\}$ of $\tilde{L}$ such that $(B(e_i, e_j)) = d\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ where $a, b, c \in \boldsymbol{Z}$, $d \in \boldsymbol{Q}^\times$, and $(a, b, c) = 1$. Since

$Q(\tilde{L}_p) \cap Z_p^\times \neq \phi$ for $p \notin S$, a prime p with $d \notin Z_p^\times$ is contained in S. Noting $Q(v) \in Z_p^\times$ for $p \in T$, we have only to prove Lemma in case that $L \cong \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, by scaling of $1/d$, and $u_p = v$ for $p \in S \cup T$. Thus we may assume that $L = Z[e_1, e_2], (B(e_i, e_j)) = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ $(a, b, c) = 1, D = b^2 - 4ac$ is not a square in Q, and $p \nmid D$ if $p \notin S$. Moreover $v \in L$ is given. By a classical theory we may suppose that a is a prime number $\notin S$ by scaling of ± 1 if necessary. Put $k = Q(\sqrt{D})$ and $\tilde{A} = Z[a, (b + \sqrt{D})/2]$, $A = (a, (b + \sqrt{D})/2)$ (= the ideal generated by a and $(b + \sqrt{D})/2$); then the norm of A is a and for $\alpha = ax + (b + \sqrt{D})y/2$ $(x, y \in Q)$, $N(\alpha) = a(ax^2 + bxy + cy^2)$. Hence $Q(xe_1 + ye_2) = N(\alpha)/a$. Thus we may consider $\tilde{A}$, $N(\alpha)/a$ as $L, Q(\alpha)$ respectively, and are given an element v in $\tilde{A}$. Put $J = (\prod_{p \in S} p)^t$; then to complete the proof we need only show that there is an element u in $\tilde{A}$ and a prime number $q \notin S$ such that $u \equiv v \bmod J$, and $Q(u) \in Z_p^\times$ for any prime $p \notin S, p \neq q$, and $Q(u) \in qZ_q^\times$. Put $(v) = BC$ where B, C are integral ideals and for a prime ideal $E | J, E | (v)$ if and only if $E | B$. Hence $(J, C) = 1$. Take a prime ideal I with a prime norm $q \notin S$ such that $I = \tilde{u}CA^{-1}, \tilde{u} \equiv 1 \bmod^\times J$. Put $u = \tilde{u}v$; then $(u) = IAB \subset A$. Hence $u \in A$, and $u \equiv v \bmod J$. Moreover $Q(u) = N(u)/a = \pm NI \cdot NB$, where $NI = q$ is a prime $\notin S$ and $NB \in Z_p^\times (p \notin S)$. We must show $u \in \tilde{A}$. Put $D = f^2 d$ where d is the discriminant of $Q(\sqrt{D})$; Since $p | J$ for $p | f, u - v = (\tilde{u} - 1)v \in fA$. $v \in \tilde{A}$ and $NA \nmid f$ imply $u \in \tilde{A}$. This completes a proof.

2. Proof of Theorem B

Without loss of generality we may assume that the scale of L is contained in Z. If $\operatorname{rank} L = 2$, then the proof of Theorem A in [1] shows that Theorem B is true. Assume $\operatorname{rank} L \geq 3$. Then take an element u_p in L_p for $p | 2dL$ such that $u_p^\perp$ is a characteristic submodule of L_p. From Lemma 3 follows that there is an element u in L and a prime $q \nmid 2dL$ such that u and u_p are sufficiently near in L_p for $p | 2dL$ and $Q(u) \in Z_p^\times$ for $p \notin S, p \neq q$, and $Q(u) \in qZ_q^\times$. Since u and u_p are sufficiently near, there is a unit $\varepsilon_p \in Z_p$ such that $Q(u) = \varepsilon_p^2 Q(u_p)$. Hence there is an isometry $\beta_p \in O(L_p)$ such that $\beta_p(u) = \varepsilon_p u_p$. Put $M = u^\perp$ in L; then M_p is a characteristic submodule of L_p $(p | 2dL)$, and $dM_q \in qZ_q^\times$, and $dM_p \in Z_p^\times$ for $p \notin S, p \neq q$. Therefore M satisfies the conditions 1),

2) in Theorem A by Lemma 2. Thus we have only to prove that $\alpha(M)$ is a direct summand of L' for an isometry α from M into a lattice L' in 2) in Theorem B. Extend α to an isometry from U to U', and put $L'' = \alpha^{-1}(L')$. Since M_p is a characteristic submodule of $L_p, L''_p = L_p$ for $p \mid 2dL$. If $p \nmid 2dL, L''_q$ is unimodular. Hence M_p is a direct summand of L''_p since $dM_p \in \boldsymbol{Z}_p^\times$ or $p\boldsymbol{Z}_p^\times$. Therefore M is a direct summand of $\alpha^{-1}(L') = L''$. This completes a proof of Theorem B.

REFERENCES

[1] Y. Kitaoka, Representations of quadratic forms and their application to Selberg's zeta functions, Nagoya Math. J. vol. **63** (1976), 153–162.
[2] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, 1963.

Department of Mathematics
Nagoya University